

07-31-00

A

JC883 U.S. PTO  
07/28/00JC864 U.S. PTO  
09/627845

07/28/00

Please type a plus sign (+) inside this box → ☐PTO/SB/05 (4/98)  
Approved for use through 09/30/2000. OMB 0651-0032  
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>UTILITY PATENT APPLICATION TRANSMITTAL</b> (Only for new nonprovisional applications under 37 C.F.R. § 1.53(b))	Attorney Docket No.	83000.1137/P4398/RSR
	First Inventor or Application Identifier	Rinaldo Di Giorgio
	Title	ADDING SECURE EXTERNAL VIRTUAL MEMORY TO SMART...
	Express Mail Label No.	EL582483120US

<b>APPLICATION ELEMENTS</b> See MPEP chapter 600 concerning utility patent application contents.		<b>ADDRESS TO:</b> Assistant Commissioner for Patents Box Patent Application Washington, DC 20231	
1. <input type="checkbox"/> * Fee Transmittal Form (e.g., PTO/SB/17) (Submit an original and a duplicate for fee processing) 2. <input checked="" type="checkbox"/> Specification [Total Pages 28] (preferred arrangement set forth below) - Descriptive title of the Invention - Cross References to Related Applications - Statement Regarding Fed sponsored R & D - Reference to Microfiche Appendix - Background of the Invention - Brief Summary of the Invention - Brief Description of the Drawings (if filed) - Detailed Description - Claim(s) - Abstract of the Disclosure 3. <input checked="" type="checkbox"/> Drawing(s) (35 U.S.C. 113) [Total Sheets 4] 4. Oath or Declaration [Total Pages ] a. <input type="checkbox"/> Newly executed (original or copy) b. <input type="checkbox"/> Copy from a prior application (37 C.F.R. § 1.63(d)) (for continuation/divisional with Box 16 completed) i. <input type="checkbox"/> DELETION OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. §§ 1.63(d)(2) and 1.33(b). * NOTE FOR ITEMS 1 & 13: IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. § 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.28).		5. <input type="checkbox"/> Microfiche Computer Program (Appendix) 6. Nucleotide and/or Amino Acid Sequence Submission (if applicable, all necessary) a. <input type="checkbox"/> Computer Readable Copy b. <input type="checkbox"/> Paper Copy (identical to computer copy) c. <input type="checkbox"/> Statement verifying identity of above copies <b>ACCOMPANYING APPLICATION PARTS</b> 7. <input type="checkbox"/> Assignment Papers (cover sheet & document(s)) 8. <input type="checkbox"/> 37 C.F.R. § 3.73(b) Statement <input type="checkbox"/> Power of Attorney (when there is an assignee) 9. <input type="checkbox"/> English Translation Document (if applicable) 10. <input type="checkbox"/> Information Disclosure <input type="checkbox"/> Copies of IDS Statement (IDS)/PTO-1449 Citations 11. <input type="checkbox"/> Preliminary Amendment 12. <input checked="" type="checkbox"/> Return Receipt Postcard (MPEP 503) (Should be specifically itemized) 13. <input type="checkbox"/> * Small Entity <input type="checkbox"/> Statement filed in prior application, Statement(s) Status still proper and desired (PTO/SB/09-12) 14. <input type="checkbox"/> Certified Copy of Priority Document(s) (if foreign priority is claimed) 15. <input type="checkbox"/> Other:	
16. If a CONTINUING APPLICATION, check appropriate box, and supply the requisite information below and in a preliminary amendment: <input type="checkbox"/> Continuation <input type="checkbox"/> Divisional <input type="checkbox"/> Continuation-in-part (CIP) of prior application No: _____ Prior application information: Examiner _____ Group / Art Unit: _____ For CONTINUATION or DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.			
<b>17. CORRESPONDENCE ADDRESS</b> <input type="checkbox"/> Customer Number or Bar Code Label <input checked="" type="checkbox"/> Correspondence address below (Insert Customer No. or Attach bar code label here)			
Name	The Hecker Law Group by Gary A. Hecker		
Address	1925 Century Park East Suite 2300		
City	Los Angeles	State	CA
Country	USA	Zip Code	90067
Telephone	310-286-0377	Fax	310-286-0488

Name (Print/Type)	Gary A. Hecker	Registration No. (Attorney/Agent)	31,023
Signature		Date	July 28, 2000

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

+

83000.1137  
P4398

UNITED STATES PATENT APPLICATION  
FOR

# ADDING SECURE EXTERNAL VIRTUAL MEMORY TO SMART CARDS

INVENTORS:

Rinaldo Di Giorgio  
Stephen Uhler  
Collin Stevens

PREPARED BY:

THE HECKER LAW GROUP  
1925 Century Park East  
Suite 2300  
Los Angeles, CA 90067

(310) 286-0377

## BACKGROUND OF THE INVENTION

### 1. FIELD OF THE INVENTION

5           The present invention relates generally to computer technology and is concerned with the use of smart cards that can be used to execute programs stored on the cards as a trusted platform. This invention relates to both hardware and software.

### 10   2. BACKGROUND ART

          A smart card is the size of a conventional credit card, and contains an electronic microchip. The chip stores electronic data and programs that are protected by security features. There are two types of smart cards, contact and  
15   contactless cards. Contact smart cards must be used in conjunction with a smart card reader. When the smart card is inserted into a smart card reader, the reader makes contact with a small gold plate about 0.5 inches in diameter on the front of the card, through which data is transferred to and from the chip. Contactless smart cards are passed near an antenna to carry out a transaction. They have an  
20   electronic microchip and an antenna embedded inside. These components allow the card to communicate with an antenna/coupler unit without physical contact.

The size of the card is determined by international standard ISO (International Standards Organization) 7810. The ISO 7810 standard defines the physical characteristics of the card, including position of the electrical contacts and how the microchip communicates with the outside world. A number of standards have also been defined for specific applications, including digital cell phones, credit card functions and electronic purses. The implementation of Java™ on smart cards is also the subject of ongoing standardization work (Javacard version 1 and 2).

There are different types of security mechanisms used in smart cards. Access to the information contained in a smart card is controlled to limit who can access the information (everybody, the card holder or a specific third party) and how can the information be accessed (read only, added to, modified or erased).

With regard to access, some smart cards require no password and anyone holding the card can have access. Others limit access to the cardholder only, typically by the use of a password in the form of a PIN (Personal Identification Number) number. If an unauthorized individual tries to use the card, it will lock-up after several unsuccessful attempts to present the correct PIN code.

Some smart cards can only be accessed by the party who issued them, as in the case of an electronic purse that can only be reloaded by the issuing bank.

Information on a smart card can be divided into information that can only be read, information that can only be added, information that can only be updated and information with no access available.

5           A smart card can restrict the use of information to an authorized person with a password. However, if this information is then transmitted by radio or telephone, additional protection is necessary. One form of protection is encryption or the use of a code. Some smart cards are capable of encryption and decryption so the stored information can be transmitted without compromising  
10 confidentiality. This authentication process ensures only genuine cards are used and makes eaves-dropping more difficult.

Some smart cards, with microprocessors and memory, have the ability to execute customized application programs. For such applications, the security of  
15 the card and its tamper resistance are of great concern. Smart cards can be used to provide additional security for applications by providing a secure tamper resistant store (or storage area) for data. Issuers of smart cards want to use the smart card memory for execution of programs because the smart card is a trusted environment.

20

One of the limitations of smart cards arises from their limited memory capacity. Current cards typically only have a few thousand bits of memory for user applications. Consequently, applications running on smart cards always tend to run out of memory. There is a need for a way to extend the memory

5 availability of smart cards to accommodate various applications.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
890  
891  
892  
893  
894  
895  
896  
897  
898  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
910  
911  
912  
913  
914  
915  
916  
917  
918  
919  
920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
930  
931  
932  
933  
934  
935  
936  
937  
938  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959  
960  
961  
962  
963  
964  
965  
966  
967  
968  
969  
970  
971  
972  
973  
974  
975  
976  
977  
978  
979  
980  
981  
982  
983  
984  
985  
986  
987  
988  
989  
990  
991  
992  
993  
994  
995  
996  
997  
998  
999  
1000  
1001  
1002  
1003  
1004  
1005  
1006  
1007  
1008  
1009  
1010  
1011  
1012  
1013  
1014  
1015  
1016  
1017  
1018  
1019  
1020  
1021  
1022  
1023  
1024  
1025  
1026  
1027  
1028  
1029  
1030  
1031  
1032  
1033  
1034  
1035  
1036  
1037  
1038  
1039  
1040  
1041  
1042  
1043  
1044  
1045  
1046  
1047  
1048  
1049  
1050  
1051  
1052  
1053  
1054  
1055  
1056  
1057  
1058  
1059  
1060  
1061  
1062  
1063  
1064  
1065  
1066  
1067  
1068  
1069  
1070  
1071  
1072  
1073  
1074  
1075  
1076  
1077  
1078  
1079  
1080  
1081  
1082  
1083  
1084  
1085  
1086  
1087  
1088  
1089  
1090  
1091  
1092  
1093  
1094  
1095  
1096  
1097  
1098  
1099  
1100  
1101  
1102  
1103  
1104  
1105  
1106  
1107  
1108  
1109  
1110  
1111  
1112  
1113  
1114  
1115  
1116  
1117  
1118  
1119  
1120  
1121  
1122  
1123  
1124  
1125  
1126  
1127  
1128  
1129  
1130  
1131  
1132  
1133  
1134  
1135  
1136  
1137  
1138  
1139  
1140  
1141  
1142  
1143  
1144  
1145  
1146  
1147  
1148  
1149  
1150  
1151  
1152  
1153  
1154  
1155  
1156  
1157  
1158  
1159  
1160  
1161  
1162  
1163  
1164  
1165  
1166  
1167  
1168  
1169  
1170  
1171  
1172  
1173  
1174  
1175  
1176  
1177  
1178  
1179  
1180  
1181  
1182  
1183  
1184  
1185  
1186  
1187  
1188  
1189  
1190  
1191  
1192  
1193  
1194  
1195  
1196  
1197  
1198  
1199  
1200  
1201  
1202  
1203  
1204  
1205  
1206  
1207  
1208  
1209  
1210  
1211  
1212  
1213  
1214  
1215  
1216  
1217  
1218  
1219  
1220  
1221  
1222  
1223  
1224  
1225  
1226  
1227  
1228  
1229  
1230  
1231  
1232  
1233  
1234  
1235  
1236  
1237  
1238  
1239  
1240  
1241  
1242  
1243  
1244  
1245  
1246  
1247  
1248  
1249  
1250  
1251  
1252  
1253  
1254  
1255  
1256  
1257  
1258  
1259  
1260  
1261  
1262  
1263  
1264  
1265  
1266  
1267  
1268  
1269  
1270  
1271  
1272  
1273  
1274  
1275  
1276  
1277  
1278  
1279  
1280  
1281  
1282  
1283  
1284  
1285  
1286  
1287  
1288  
1289  
1290  
1291  
1292  
1293  
1294  
1295  
1296  
1297  
1298  
1299  
1300  
1301  
1302  
1303  
1304  
1305  
1306  
1307  
1308  
1309  
1310  
1311  
1312  
1313  
1314  
1315  
1316  
1317  
1318  
1319  
1320  
1321  
1322  
1323  
1324  
1325  
1326  
1327  
1328  
1329  
1330  
1331  
1332  
1333  
1334  
1335  
1336  
1337  
1338  
1339  
1340  
1341  
1342  
1343  
1344  
1345  
1346  
1347  
1348  
1349  
1350  
1351  
1352  
1353  
1354  
1355  
1356  
1357  
1358  
1359  
1360  
1361  
1362  
1363  
1364  
1365  
1366  
1367  
1368  
1369  
1370  
1371  
1372  
1373  
1374  
1375  
1376  
1377  
1378  
1379  
1380  
1381  
1382  
1383  
1384  
1385  
1386  
1387  
1388  
1389  
1390  
1391  
1392  
1393  
1394  
1395  
1396  
1397  
1398  
1399  
1400  
1401  
1402  
1403  
1404  
1405  
1406  
1407  
1408  
1409  
1410  
1411  
1412  
1413  
1414  
1415  
1416  
1417  
1418  
1419  
1420  
1421  
1422  
1423  
1424  
1425  
1426  
1427  
1428  
1429  
1430  
1431  
1432  
1433  
1434  
1435  
1436  
1437  
1438  
1439  
1440  
1441  
1442  
1443  
1444  
1445  
1446  
1447  
1448  
1449  
1450  
1451  
1452  
1453  
1454  
1455  
1456  
1457  
1458  
1459  
1460  
1461  
1462  
1463  
1464  
1465  
1466  
1467  
1468  
1469  
1470  
1471  
1472  
1473  
1474  
1475  
1476  
1477  
1478  
1479  
1480  
1481  
1482  
1483  
1484  
1485  
1486  
1487  
1488  
1489  
1490  
1491  
1492  
1493  
1494  
1495  
1496  
1497  
1498  
1499  
1500  
1501  
1502  
1503  
1504  
1505  
1506  
1507  
1508  
1509  
1510  
1511  
1512  
1513  
1514  
1515  
1516  
1517  
1518  
1519  
1520  
1521  
1522  
1523  
1524  
1525  
1526  
1527  
1528  
1529  
1530  
1531  
1532  
1533  
1534  
1535  
1536  
1537  
1538  
1539  
1540  
1541  
1542  
1543  
1544  
1545  
1546  
1547  
1548  
1549  
1550  
1551  
1552  
1553  
1554  
1555  
1556  
1557  
1558  
1559  
1560  
1561  
1562  
1563  
1564  
1565  
1566  
1567  
1568  
1569  
1570  
1571  
1572  
1573  
1574  
1575  
1576  
1577  
1578  
1579  
1580  
1581  
1582  
1583  
1584  
1585  
1586  
1587  
1588  
1589  
1590  
1591  
1592  
1593  
1594  
1595  
1596  
1597  
1598  
1599  
1600  
1601  
1602  
1603  
1604  
1605  
1606  
1607  
1608  
1609  
1610  
1611  
1612  
1613  
1614  
1615  
1616  
1617  
1618  
1619  
1620  
1621  
1622  
1623  
1624  
1625  
1626  
1627  
1628  
1629  
1630  
1631  
1632  
1633  
1634  
1635  
1636  
1637  
1638  
1639  
1640  
1641  
1642  
1643  
1644  
1645  
1646  
1647  
1648  
1649  
1650  
1651  
1652  
1653  
1654  
1655  
1656  
1657  
1658  
1659  
1660  
1661  
1662  
1663  
1664  
1665  
1666  
1667  
1668  
1669  
1670  
1671  
1672  
1673  
1674  
1675  
1676  
1677  
1678  
1679  
1680  
1681  
1682  
1683  
1684  
1685  
1686  
1687  
1688  
1689  
1690  
1691  
1692  
1693  
1694  
1695  
1696  
1697  
1698  
1699  
1700  
1701  
1702  
1703  
1704  
1705  
1706  
1707  
1708  
1709  
1710  
1711  
1712  
1713  
1714  
1715  
1716  
1717  
1718  
1719  
1720  
1721  
1722  
1723  
1724  
1725  
1726  
1727  
1728  
1729  
1730  
1731  
1732  
1733  
1734  
1735  
1736  
1737  
1738  
1739  
1740  
1741  
1742  
1743  
1744  
1745  
1746  
1747  
1748  
1749  
1750  
1751  
1752  
1753  
1754  
1755  
1756  
1757  
1758  
1759  
1760  
1761  
1762  
1763  
1764  
1765  
1766  
1767  
1768  
1769  
1770  
1771  
1772  
1773  
1774  
1775  
1776  
1777  
1778  
1779  
1780  
1781  
1782  
1783  
1784  
1785  
1786  
1787  
1788  
1789  
1790  
1791  
1792  
1793  
1794  
1795  
1796  
1797  
1798  
1799  
1800  
1801  
1802  
1803  
1804  
1805  
1806  
1807  
1808  
1809  
1810  
1811  
1812  
1813  
1814  
1815  
1816  
1817  
1818  
1819  
1820  
1821  
1822  
1823  
1824  
1825  
1826  
1827  
1828  
1829  
1830  
1831  
1832  
1833  
1834  
1835  
1836  
1837  
1838  
1839  
1840  
1841  
1842  
1843  
1844  
1845  
1846  
1847  
1848  
1849  
1850  
1851  
1852  
1853  
1854  
1855  
1856  
1857  
1858  
1859  
1860  
1861  
1862  
1863  
1864  
1865  
1866  
1867  
1868  
1869  
1870  
1871  
1872  
1873  
1874  
1875  
1876  
1877  
1878  
1879  
1880  
1881  
1882  
1883  
1884  
1885  
1886  
1887  
1888  
1889  
1890  
1891  
1892  
1893  
1894  
1895  
1896  
1897  
1898  
1899  
1900  
1901  
1902  
1903  
1904  
1905  
1906  
1907  
1908  
1909  
1910  
1911  
1912  
1913  
1914  
1915  
1916  
1917  
1918  
1919  
1920  
1921  
1922  
1923  
1924  
1925  
1926  
1927  
1928  
1929  
1930  
1931  
1932  
1933  
1934  
1935  
1936  
1937  
1938  
1939  
1940  
1941  
1942  
1943  
1944  
1945  
1946  
1947  
1948  
1949  
1950  
1951  
1952  
1953  
1954  
1955  
1956  
1957  
1958  
1959  
1960  
1961  
1962  
1963  
1964  
1965  
1966  
1967  
1968  
1969  
1970  
1971  
1972  
1973  
1974  
1975  
1976  
1977  
1978  
1979  
1980  
1981  
1982  
1983  
1984  
1985  
1986  
1987  
1988  
1989  
1990  
1991  
1992  
1993  
1994  
1995  
1996  
1997  
1998  
1999  
2000  
2001  
2002  
2003  
2004  
2005  
2006  
2007  
2008  
2009  
2010  
2011  
2012  
2013  
2014  
2015  
2016  
2017  
2018  
2019  
2020  
2021  
2022  
2023  
2024  
2025  
2026  
2027  
2028  
2029  
2030  
2031  
2032  
2033  
2034  
2035  
2036  
2037  
2038  
2039  
2040  
2041  
2042  
2043  
2044  
2045  
2046  
2047  
2048  
2049  
2050  
2051  
2052  
2053  
2054  
2055  
2056  
2057  
2058  
2059  
2060  
2061  
2062  
2063  
2064  
2065  
2066  
2067  
2068  
2069  
2070  
2071  
2072  
2073  
2074  
2075  
2076  
2077  
2078  
2079  
2080  
2081  
2082  
2083  
2084  
2085  
2086  
2087  
2088  
2089  
2090  
2091  
2092  
2093  
2094  
2095  
2096  
2097  
2098  
2099  
2100  
2101  
2102  
2103  
2104  
2105  
2106  
2107  
2108  
2109  
2110  
2111  
2112  
2113  
2114  
2115  
2116  
2117  
2118  
2119  
2120  
2121  
2122  
2123  
2124  
2125  
2126  
2127  
2128  
2129  
2130  
2131  
2132  
2133  
2134  
2135  
2136  
2137  
2138  
2139  
2140  
2141  
2142  
2143  
2144  
2145  
2146  
2147  
2148  
2149  
2150  
2151  
2152  
2153  
2154  
2155  
2156  
2157  
2158  
2159  
2160  
2161  
2162  
2163  
2164  
2165  
2166  
2167  
2168  
2169  
2170  
2171  
2172  
2173  
2174  
2175  
2176  
2177  
2178  
2179  
2180  
2181  
2182  
2183  
2184  
2185  
2186  
2187  
2188  
2189  
2190  
2191  
2192  
2193  
2194  
2195  
2196  
2197  
2198  
2199  
2200  
2201  
2202  
2203  
2204  
2205  
2206  
2207  
2208  
2209  
2210  
2211  
2212  
2213  
2214  
2215  
2216  
2217  
2218  
2219  
2220  
2221  
2222  
2223

## SUMMARY OF THE INVENTION

In one or more embodiments of the invention, a Smart Card URL Programming interface (UPI) builds a local web or card server around a card terminal and the inserted smart card. This server can also support secure object storage, which stores serialized, secure signed, compressed objects (or applications or data) for delivery to the card or for off-loading from the card. The secure object storage is also web addressable, so that a user needs only one storage area that can be on the Internet and accessed from all locations. The object storage program stores objects with the option of signing and/or encrypting and retrieves objects which may require cryptographic credentials.

If a user desires to run applications on a card that exceed the memory capacity of the card, information about the applications, including pointers and their digital signatures, is acquired and stored on the card by the card server. The card is thus provided with basic information about the nature of the applications that are authorized for use on the card at the time that the card is first loaded. The applications on a card and their movement on and off the card are managed by the card server. Applications on a card can be moved off to secure storage and applications in secure storage can be moved to the smart card.

Data on a card can be moved to secure storage and data in secure storage can be moved to the card securely.

83000.1137 P/4398



## BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 illustrates some of the features of an embodiment of a smart card.

- 5    Figure 2 illustrates some of the components of an embodiment of a smart card server and smart card reader/writer terminal.

Figure 3 illustrates some of the steps of an embodiment of the process for placing applications on a smart card initially.

10

Figure 4 illustrates some of the steps of an embodiment of the process for removing and replacing applications on a smart card.

- 15    Figure 5 illustrates an example of a general-purpose computer that can be used to implement an embodiment of this invention as computer software in the form of computer readable program code.

## DETAILED DESCRIPTION OF THE INVENTION

A method and apparatus for adding secure external memory to smart cards is described. In the following description, numerous specific details are set forth in order to provide a more thorough description of the present invention. It will be apparent, however, to one skilled in the art, that the present invention may be practiced without these specific details. In other instances, well-known features have not been described in detail so as not to obscure the invention.

10 An embodiment of the invention can be implemented as computer software in the form of computer readable program code executed on one or more general-purpose computers such as the computer 500 illustrated in Figure 5. A keyboard 510 and mouse 511 are coupled to a bi-directional system bus 518 (e.g., PCI, ISA or other similar architecture). The keyboard and mouse are for  
15 introducing user input to the computer system and communicating that user input to central processing unit (CPU) 513. Other suitable input devices may be used in addition to, or in place of, the mouse 511 and keyboard 510. I/O (input/output) unit 519 coupled to bi-directional system bus 518 represents possible output devices such as a printer or an A/V (audio/video) device.

20

Computer 500 includes video memory 514, main memory 515, mass storage 512, and communication interface 520. All these devices are coupled to a bi-directional system bus 518 along with keyboard 510, mouse 511 and CPU 513.

The mass storage 512 may include both fixed and removable media, such as

5 magnetic, optical or magnetic optical storage systems or any other available mass storage technology. The system bus 518 provides a means for dressing video

memory 514 or main memory 515. The system bus 515 also provides a

mechanism for the CPU to transfer data between and among the components,

such as main memory 515, video memory 514 and mass storage 512. In one

10 embodiment of the invention, the CPU 513 is a microprocessor manufactured by

Motorola, such as the 650X0 processor, an Intel Pentium III processor, or an

UltraSparc processor from Sun Microsystems. However, any other suitable

processor or computer may be utilized. Video memory 514 is a dual-ported

video random access memory. One port of the video memory 514 is coupled to

15 video accelerator or video amplifier 516. The video accelerator device 516 is used

to drive a CRT (cathode ray tube), and LCD (Liquid Crystal Display), or TFT

(Thin-Film Transistor) monitor 517. The video accelerator 516 is well known in

the art and may be implemented by any suitable apparatus. This circuitry

converts pixel data stored in video memory 514 to a signal suitable for use by

20 monitor 517. The monitor 517 is a type of monitor suitable for displaying

graphic images.

The computer 500 may also include a communication interface 520 coupled to the system bus 518. The communication interface 520 provides a two-way data communication coupling via a network link 521 to a network 522. For example, if the communication interface 520 is a modem, the communication interface 520 provides a data communication connection to a corresponding type of telephone line, which comprises part of a network link 521. If the communication interface 520 is a Network Interface Card (NIC), communication interface 520 provides a data communication connection via a network link 521 to a compatible network. Physical network links can include Ethernet, wireless, fiber optic, and cable television type links. In any such implementation, communication interface 520 sends and receives electrical, electromagnetic or optical signals, which carry digital data streams representing various types of information.

The network link 521 typically provides data communication through one or more networks to other data devices. For example, network link 521 may provide a connection through local network 522 to a host computer 523 or to data equipment operated by an Internet Service Provider (ISP) 524. ISP 524 in turn provides data communication services through the world wide packet data communication network now commonly referred to as the "Internet" 525. Local

network 522 and Internet 525 both use electrical, electromagnetic or optical signals that carry digital data streams to files. The signals through the various networks and the signals on network link 521 and through communication interface 520, which carry the digital data to and from computer 500, are  
5 exemplary forms of carrier waves for transporting the digital information.

The computer 500 can send messages and receive data, including program code, through the network(s), network link 521, and communication interface 520. In the Internet example, server 526 might transmit a requested code for an  
10 application program through Internet 525, ISP 524, local network 522 and communication interface 520.

The computer system described above is for purposes of example only. An embodiment of the invention may be implemented in any type of computer  
15 system or programming or processing environment.

Smart cards are of interest because they can be used to provide additional security for applications and data by providing a secure, tamper resistant storage area for applications and data. The memory that can be placed on a smart card is  
20 limited and, consequently, applications using smart cards tend to run out of memory. There is a need for a way to extend the memory available to smart

cards (and other portable device with limited memory capacity) to accommodate various applications. In order to run applications in the memory of a smart card, identifiers must be provided to locate the desired applications or data from another source that might be a network or any other location where data can be  
5 stored. In one embodiment of this invention, a URL (Uniform Resource Locator) Programming Interface (UPI) is used to provide identifying information to identify and locate applications and data. The URL Programming Interface will now be discussed in greater detail for one embodiment of this invention.

10       Developing consistent, reliable Web applications that interface to different devices--such as home networks, home automation systems, or real-time process control devices -- may be simplified by treating devices as URLs. The URL programming interface (UPI) provides a set of URLs for a device that are available to any application capable of performing the HTTP (HyperText  
15 Transfer Protocol). HTTP has become so universal that in college computer courses students are often given as an assignment the creation of an HTTP stack. This trend is due to the growing interest in connecting devices to the Internet. Sun Microsystems Laboratories has used the Java™ language to develop a technology that allows users to deploy very small HTTP stacks, with a core of  
20 less than 100 KB. However, the claimed invention can be practiced using any computer programming language.

These small HTTP servers can be run on any embedded device or used as application servers that are similar to traditional Web servers. Such minimal servers provide an integrated presentation and service layer for a device.

5 Because a Web server answers URL requests, universal access to devices from any Internet node is achieved. UPI provides an interface to allow applications, including web applications, to access any device as if the device is a file resident on a web server, if the device can perform the HTTP protocol.

10 The UPI architecture, at its core, consists of a series of handlers that are similar to servlets, but have fewer features. These handlers are mapped to incoming URL requests. This allows the UPI function on very small devices, such as a TINI board. The UPI supplies handlers for web services such as file service and CGI script execution. Application developers can develop handlers  
15 for Internet aware devices (IADs) simply by coding a few required methods, such as *init* and *respond*, along with code that understands the applicable device grammar.

Figure 1 illustrates some of the features of one embodiment of a smart  
20 card. In Figure 1, smart card 100 includes a contact 110 to transfer information to a smart card reader and an electronic microchip 120. As discussed earlier,

applications running on smart cards tend to have a limited memory capacity.

There is a need for a way to extend the memory available to smart cards to accommodate various applications. For example, in a credit card environment, a user may wish to maintain accounts with a dozen or more vendors, such as

5 airlines, car rental companies and hotel chains and use his smart card as a means of payment at all of them. This usage requires considerably more memory than a typical smart card has available. The smart card may have the capability of storing data for several accounts, but not for a dozen accounts. In order to extend the memory capability of a smart card to accommodate such applications, 10 a secure virtual paging system is implemented for data and instructions, or programs, in this invention. Instructions are additional programs and data refers to additional personal/corporate information like the birthdays of people or all the access mechanisms for controlled web sites.

15 In this invention, the Smart Card URL (Uniform Resource Locator) Programming Interface (UPI) builds a local web or card server around a card terminal and the inserted smart card. Figure 2 illustrates some of the components of an embodiment of a smart card server and smart card reader/writer terminal. In Figure 2, smart card 100 is shown in the smart card 20 reader 200 connected by a cable 220, or in some other way, to card server 210. This server can also support secure object storage, which stores serialized, secure,



signed, compressed objects for delivery to the card or for off-loading from the card. The secure object storage is also web addressable, so that a user needs only one storage area that can be on the Internet and accessed from all locations.

These operations are performed by an object storage program that stores an

5 object with the option of signing and or encrypting and retrieves an object which may be encrypted.

If a user desires to run a number of applications on a card that exceeds the card's memory capacity, information about the applications, including identifiers  
10 or pointers and their digital signatures, is acquired and stored on the smart card by the card server. The card is thus provided with basic information about the nature of the applications that are authorized for use on the card at the time that the card is first loaded. The card server may manage the applications on a card and their movement on and off the card. However, the invention contemplates  
15 the use of any other component configured to manage the movement of such applications. Applications on a card can be moved off to secure storage and applications in secure storage can be moved to the smart card. Data on a card can be moved to secure storage and data in secure storage can be moved to the card securely. However, the applications (e.g., computer readable program code)  
20 can also be stored in a non-secure environment or an environment having limited security.

Data or authorized applications in secure storage may be signed using a signature algorithm, such as DSS (Digital Signature Standard, a National Institute of Standards and Technology proposed standard for digital signatures using a public key digital signature algorithm) or a custom solution using SHA-1 (Secure Hash Algorithm 1, a hash algorithm developed by the National Institute of Standards and Technology and the National Security Agency). The secret key for the storage is recorded on the card and all signing operations are performed on the smart card. Typically these objects are small, so that all encryption and decryption operations are also performed on the card. This invention allows trusted code to be always run on the card. The invention manages applications on the cards and performs encryption and decryption while loading and unloading data and program segments. The smart card is tamper resistant and the card participates in signing the applications so that the security for the system resides in the smart card. Applications intended for use may be routed through the card which signs them before they are stored at the secure storage area.

The card is provided with a look up table (e.g., a series of pointer) that contains the name of the application, the location in the form of a URL and a checksum. A checksum, or hash, is a count of the number of bits in a

transmission unit so that the recipient can make sure the correct number of bits arrived and that the message is intact. When the user wants applications, the card server obtains the applications and records them on the card if the card is authorized to use them. The card server (or some other component) allows the

5 application to execute on the card if it passes the required verification. This system avoids the need of having to go to the application's manufacturer to load an application on the card. It is possible to have a personal library for the card stored for use as needed on the card server. Any card reader that is network enabled with the appropriate technology (e.g., UPI) can fetch and load  
10 applications transparently to the user. Applications can be ranked according to frequency of use for faster operation.

Figure 3 illustrates some of the steps of the process for placing applications on a smart card initially in one embodiment of this invention. In  
15 Figure 3, the user initially selects the applications desired at step 300 and their priority for placement on the smart card. A command is sent to the card sever to process the selected applications at step 310. At step 320, the card server determines if the applications selected will fit within the memory constraints of the smart card. If the applications selected will fit on the smart card, the process  
20 proceeds to step 330 and then to step 335 where instructions are issued to the smart card reader/writer terminal to write the applications on the card at step

340. At step 345, the user runs the selected applications on the smart card and obtains the desired result 350.

If the applications selected will not fit on the smart card, the process  
5 proceeds to sep 360 and then to step 365. At step 365, instructions are issued to the smart card reader/writer terminal that will be later written on the smart card. These instructions include (1) notice that only some applications can be placed on the smart card, (2) identification of all selected applications that will eventually be used together with authorizations for their use and (3) the  
10 applications that will be written on the card initially. At step 375, the smart card reader writer terminal writes all of this information on the smart card. At step 380, the user runs the selected applications on the smart card and obtains the desired result 385. At the same time that step 365 is being processed, the selected applications that cannot be written on the smart card, due to memory  
15 constraints, are stored on the secure card server at step 390.

Figure 4 illustrates some of the steps, in one embodiment of this invention, of the process for removing and replacing some of the applications on a smart card that was loaded with applications earlier, as described in the discussion of  
20 Figure 3. In Figure 4, the user selects applications that have been authorized, but not recorded, on the smart card at step 400. At step 405, the terminal

communicates with the smart card to determine authorized applications. At step 410, the smart card uses information recorded on the smart card at the time of initial use, identifying applications that eventually would be needed and are authorized for use. The smart card reports this information back to the card server requesting transmission of the applications. The card sever examines the request from the smart card and determines whether to process the selected applications for placement on the smart card at step 420. At step 430, the card server determines if the applications selected will fit within the memory constraints of the smart card. If the applications selected will fit on the smart card, the process proceeds to sep 440 and then to step 445 where instructions are issued to the smart card reader/writer terminal to write the applications on the card at step 455. At step 460, the user runs the selected applications on the smart card and obtains the desired result 465.

If the applications selected will not fit on the smart card, the process proceeds to sep 470 and then to step 475. At step 475, instructions are issued to the smart card reader writer terminal to remove unneeded applications and data. These are sent to the card server at step 500 for secure storage where they can be retrieved later by the smart card. Other applications that will be needed later that will not fit on the smart card are also sent in step 500 to the card server for secure storage. At step 480, the smart card reader/writer terminal is sent

information on the requested applications. At step 485, the smart card reader/writer terminal writes all of this information on the smart card. At step 490, the user runs the selected applications on the smart card and obtains the desired result 495.

5

In the event that the user selects applications that have not been previously authorized, then access to these applications will be declined and the user will have to repeat the process described in Figure 3 in order to obtain the new applications.

10

## CLAIMS

What is claimed is:

1. An apparatus comprising:

a portable device having a processor and memory coupled to said

5 processor;

a pointer residing in said memory, said pointer identifying the  
location of data;

an interface to said portable device wherein said interface is  
configured to transmit data to said memory of said portable device when said

10 portable device requests said data.

2. The apparatus of claim 1 wherein said portable device comprises a smart  
card.

15 3. The apparatus of claim 1 wherein said computer readable environment is  
stored in a secure environment.

4. The apparatus of claim 1 wherein said data comprises computer readable  
program code.

20

5. The apparatus of claim 1 wherein said interface determines if said

portable device is authorized to access said data prior to transmitting said data to said portable device.

6. A method for adding external memory to a portable device comprising:

5 storing at least one identifier wherein said identifier comprises a location of data;

determining if a portable device having memory has access to said data;

10 determining if said memory has sufficient capacity to store said data;

obtaining said data from a data source using said at least one identifier.

7. The method of claim 6 further comprising:

15 storing a private key associated with said data in said memory of said portable device.

8. The method of claim 6 wherein said portable device comprises a smart card.

9. The method of claim 8 wherein said smart card interfaces with a smart



card server.

10. The method of claim 6 further comprising:  
obtaining a private key from said memory of said smart card.

5

11. The method of claim 10 further comprising:  
determining if said private key complements a public key;  
permitting access to said data residing on said data source.

- 10 12. The method of claim 6 wherein said determining if said memory has  
sufficient capacity to store said data further comprises:  
clearing space for said data when said memory is full.

- ~~13.~~ A computer program product comprising:  
15 a computer readable medium having computer readable program code  
embodied therein, said computer readable program code configured to:

store at least one identifier wherein said identifier comprises a  
location of data;

determine if a portable device having memory has access to said

20 data;

determine if said memory has sufficient capacity to store said data;

obtain said data from a data source using said at least one  
identifier.

14. The computer program product of claim 13 further comprising computer  
5 readable program code configured to:

store a private key associated with said data in said memory of said  
portable device.

15. The computer program product of claim 13 wherein said portable device  
10 comprises a smart card.

16. The computer program product of claim 15 wherein said smart card  
interfaces with a smart card server.

15 17. The computer program product of claim 15 further comprising computer  
readable program code configured to:

obtain a private key from said memory of said smart card.

18. The computer program product of claim 17 further comprising computer  
20 readable program code configured to:

determine if said private key complements a public key;

permit access to said data residing on said data source.

19. The computer readable program code of claim 14 wherein said  
determining if said memory has sufficient capacity to store said data further

5 comprises computer readable program code configured to:

clear space for said data when said memory is full.

~~20.~~ A method for adding external memory to a smart card comprising:

storing information required by a smart card on a smart card server;

10 transferring data comprising applications for processing on said smart  
card and authorizations and encryption keys for other applications from said  
smart card server through a cable to a smart card terminal capable of reading  
and writing to said smart card;

transferring said data from said smart card terminal to said smart card

15 through an electrical contact on said smart card;

storing said data on said smart card for processing on said smart card;

processing said data on said smart card for a user;

issuing a request for additional applications as need by said user for  
transfer to said smart card together with encryption keys;

20 authentication and authorization of said request by said smart card server  
using data on said smart card;



## ABSTRACT OF THE DISCLOSURE

The Smart Card URL Programming interface (UPI) builds a local web or card server around a card terminal and the inserted smart card. This server can also support secure object storage, which stores serialized, secure signed,  
5 compressed objects (or applications or data) for delivery to the card or for off-loading from the card. The secure object storage is also web addressable, so that a user needs only one storage area that can be on the Internet and accessed from all locations. The object storage program stores objects with the option of signing and/or encrypting and retrieves objects which may require cryptographic  
10 credentials.

If a user desires to run applications on a card that exceed the memory capacity of the card, information about the applications, including pointers and their digital signatures, is acquired and stored on the card by the card server.

15 The card is thus provided with basic information about the nature of the applications that are authorized for use on the card at the time that the card is first loaded. The card server manages the applications on a card and their movement on and off the card. Applications on a card can be moved off to secure storage and applications in secure storage can be moved to the smart card.  
20 Data on a card can be moved to secure storage and data in secure storage can be moved to the card securely.

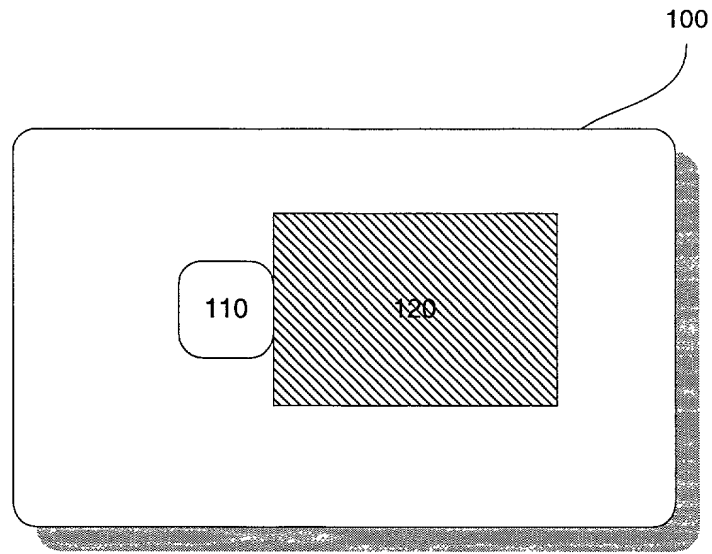


FIG. 1

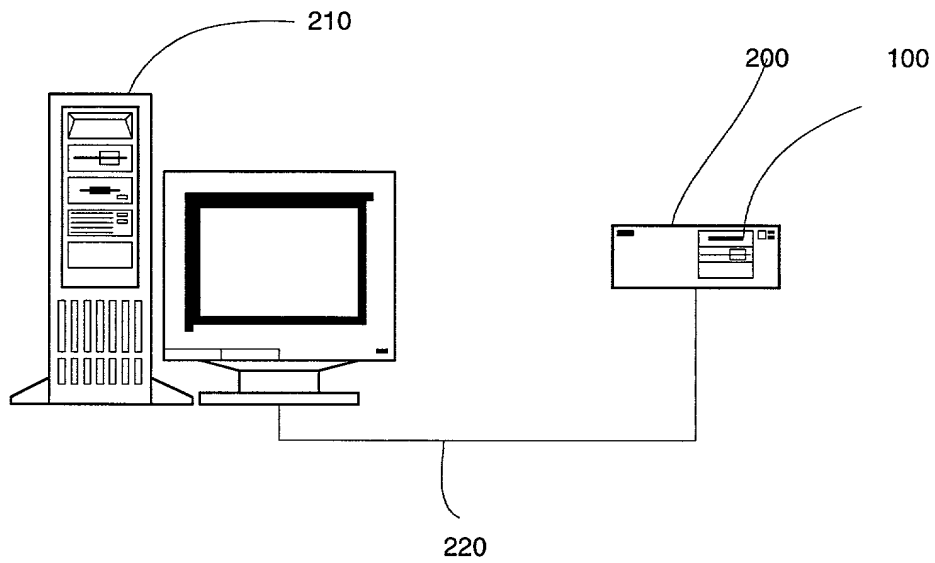


FIG. 2

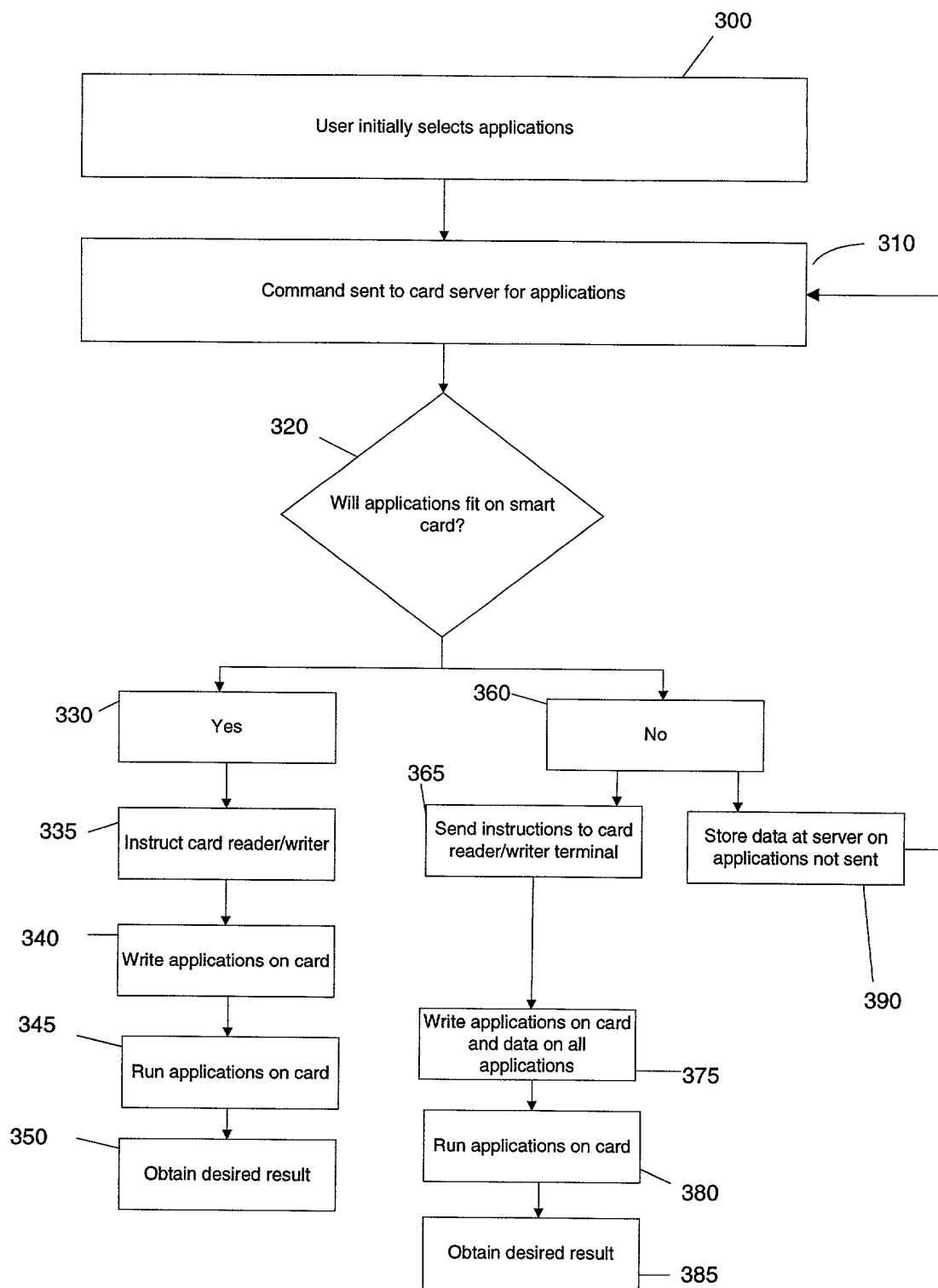
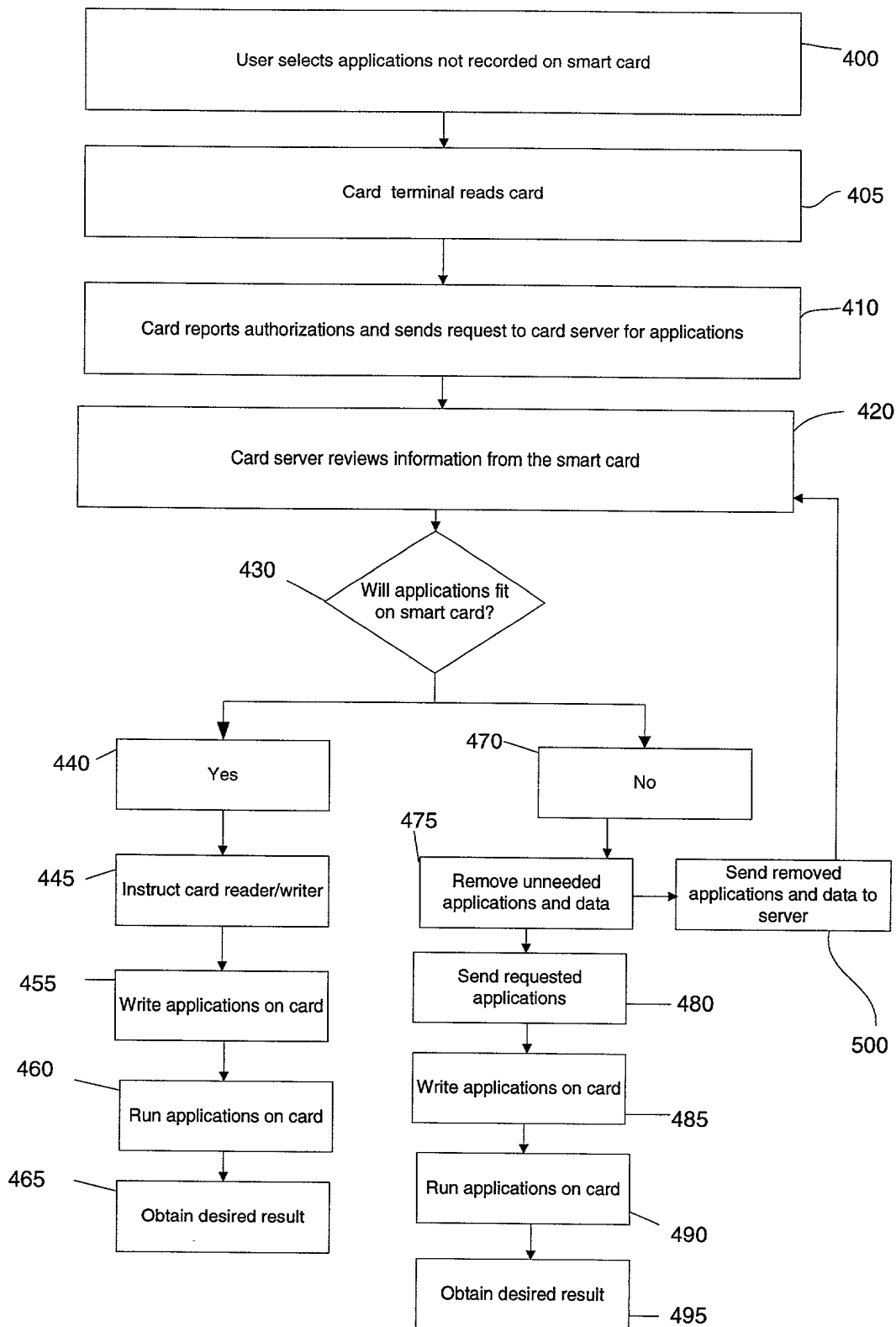


FIG. 3



**FIG. 4**



FIG. 5 is a block diagram of a computer system 500 in accordance with the present invention. The system 500 includes a processor 513, a main memory 515, a video memory 514, a video amplifier 516, a CRT 517, a keyboard 510, a mouse 511, a mass storage 512, a communication interface 520, and an I/O 519. The processor 513 is connected to the main memory 515, the video memory 514, the keyboard 510, and the mouse 511. The video memory 514 is connected to the video amplifier 516, which is connected to the CRT 517. The mass storage 512 is connected to the communication interface 520. The communication interface 520 is connected to a network link 521, which is connected to a local network 522. The local network 522 is connected to an Internet service provider (ISP) 524, which is connected to the Internet 525. The Internet 525 is connected to a server 526.

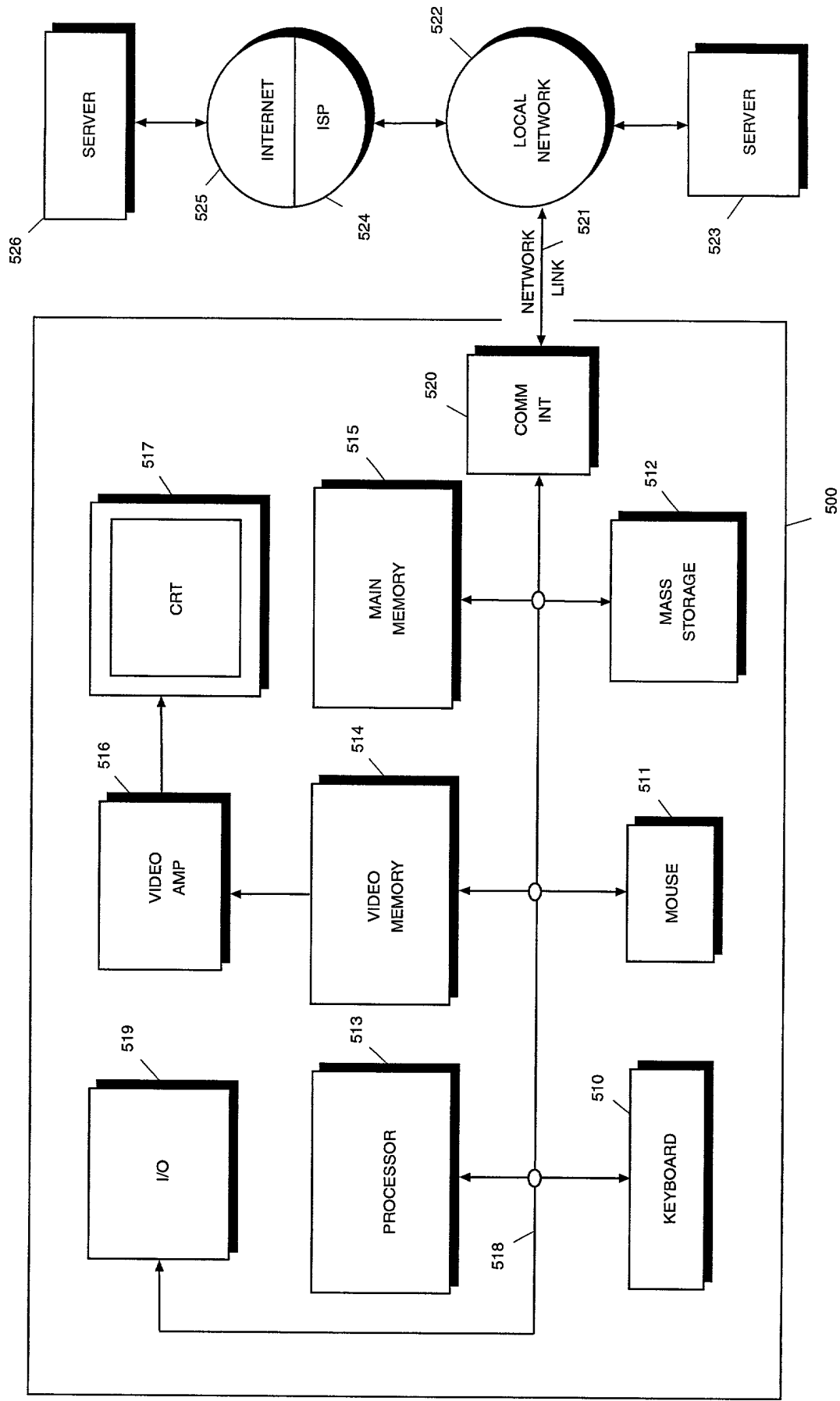


FIGURE 5